UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,124	02/12/2002	Lee Ming Cheng	P-370.240	7727

7590 07/07/2005

JACKSON WALKER L.L.P.
Suite 2100
112 E. Pecan Street
San Antonio, TX 78205

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/074,124	CHENG ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 June 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 2/12/2002.

Specification

2. The disclosure is objected to because of the following informalities: (a) the phrase "the same input will be obtained" as shown in paragraph 5 should be "the same output will be obtained", (b) The sentence "The length is of the n LFSRs 18 are pairwise relatively prime ...", as shown in paragraph 33 has incorrect English grammar by using two verbs, and (c) the phrase "Periodic Sequence Generator 11 has a period of π..." has incorrect notation and subscript as well (not the 3.1416's "pi"). See 37 CFR 1.71. Appropriate correction is required.

Drawings

The drawings are objected to because of the following informalities: (a) Figure 1 should have K2 associated with MUX2 instead of K1 and (b) Figure 5 shows unclear connection between R4 and R5.

A proposed drawing correction or corrected drawings are required in reply to the Office Action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 7 is rejected under 35 U.S.C. 101 because the claimed subject matter is not technologically embodied which is just an abstract idea and is therefore the claim is directed to non-statutory subject matter as not being tangible.

Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 and 2 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitation of claims 1 and 2 recites the switches and controller; however, it is not enabled by the specification regarding how to form the first output of K1 (and K2) of the controller from the bit stream pointed out at a particular shift register R_n as another form of input to the corresponding MUX. Examiner requests a more clear

specification should be provided. Any other claims not addressed are rejected by virtue of their dependency

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> **The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.**

4. Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 is indefinite because the claim language "the first generator" has insufficient antecedent basis for this limitation in the claim as to either per sequence generator or per nonlinear function generator.

Any other claims not addressed are rejected by virtue of their dependency

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 7, 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roth (Patent Number: 5243650), in view of Beker (Patent Number: 4748576).

As per claim 7, Roth teaches a method of generating a pseudo random sequence for random number generation or a stream cipher engine including generating a first plurality of binary sequences, applying a plurality of nonlinear functions to said first plurality of binary sequences to obtain an uncorrelated second plurality of binary sequences (Roth: Figure 5);

Roth does not disclose expressly randomly selecting an output sequence from one of the second plurality of binary sequences.

Beker teaches randomly selecting an output sequence from one of the second plurality of binary sequences (Beker: Figure 1; Roth: Figure 5)

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Beker within the system of Roth because Beker teaches providing a more secure pseudo-random binary sequence generators that can reduce the possibilities of mimicking the generator output and thus increase the unpredictability of both the output signal even the contents of some of the shift register stages may be known (Beker: Column 1 Line 26 – 31).

As per claim 8, Roth further teaches the nonlinear functions are arranged to provide a one-to-many relationship between the first and second plurality of binary sequences (Roth: Figure 5).

As per claim 9, Roth further teaches the nonlinear functions are boolean functions (Roth: Column 3 Line 46 – 52 & Claim-4: the nonlinear functions comprises a XOR adder from a plurality of LFSRs and a nonlinear shift register).

6. Claims 1 – 6 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beker (Patent Number: 4748576), in view of Roth (Patent Number: 5243650), and in view of Puhl (Patent Number: 5365585).

As per claim 1 and 2, Roth teaches a sequence generator including:

a plurality of linear feedback shift registers operable to generate a plurality of binary sequences (Beker: Figure 1),

at least first and second switches (Beker: Figure 1 and Figure 3: MUX is equivalent to a switch and Beker discloses 1st MUX (Figure 1) represented as the second switch and 2nd MUX (Figure 3) represented as the first switch);

a controller including a shift register operable to control said first and second switches (Beker: Figure 1 and Figure 3: the controller of Figure 1 is on the LEFT of the figure and the controller of Figure 3 is on the TOP of the figure);

the second switch operative to select one of said second plurality of binary sequences to an output (Beker: Figure 1: select one out of 32 of a plurality of binary sequences to an output);

Beker does not disclose expressly a plurality of nonlinear functions having said binary sequences as their input and operable to generate a second plurality of binary sequences;

Roth teaches a plurality of nonlinear functions having said binary sequences as their input and operable to generate a second plurality of binary sequences (Roth: Figure 5, Column 3 Line 46 – 52 and Claim-4: the nonlinear functions comprises XOR adder from a plurality of LFSRs as well as a nonlinear feedback shift register);

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Roth within the system of Beker because Roth teaches providing an effective encryption mechanism by using a pseudo random binary sequence generated with a nonlinear feedback register initialized by a control word where the control word in turn is generated by a true random sequence generator (Roth: Abstract).

Beker as modified does not disclose expressly the first switch operative to select one of said second plurality of binary sequences to the first bit of the shift register.

Puhl teaches the first switch operative to connect / apply the output of switch into the first bit of the shift register (Puhl: Figure 2 Element 268).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Puhl within the system of Roth as modified because Puhl teaches providing a more secure pseudo-random binary sequence generators by using an internal control mechanism which is easy to implement (Puhl: Column 1 – 3 and Column 5 Line 34 – 37).

Accordingly, Becker as modified teaches the first switch operative to select one of said second plurality of binary sequences to the first bit of the shift register (Puhl: Figure 2 Element 268; Beker: Figure 3: connecting the output of switch / MUX into the input of controller – i.e. LOAD signal as shown in Beker's Figure 3; Roth: Figure 5).

As per claim 3, Roth further teaches the sequence generator includes a plurality of feedback shift registers each operable to generate a binary sequence (Roth: Figure 5).

As per claim 4, Roth further teaches the nonlinear function generators includes a plurality of boolean functions, each boolean function having the first plurality of binary sequences as an input and being operable to generate a binary sequence (Roth: Column 3 Line 46 – 52 & Claim-4: the nonlinear functions comprises a XOR adder from a plurality of LFSRs and a nonlinear shift register).

As per claim 5, Beker further teaches the switches are multiplexers (Beker: Figure 1).

As per claim 6, Roth as modified further teaches the controller includes a shift register, the input of the controller being the first bit of the register and the outputs of the controller being at positions along the register (Puhl: Figure 2 Element 268; Beker:

Figure 3: connecting the output of switch / MUX into the input of controller – i.e. LOAD signal as shown in Beker's Figure 3; Roth: Figure 5).

As per claim 10, Roth as modified does not teach the output sequence is randomly selected by applying one of the second plurality of binary sequences to a shift register.

Puhl teaches the first switch operative to connect / apply the output of switch into the first bit of the shift register (Puhl: Figure 2 Element 268).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Puhl within the system of Roth as modified because Puhl teaches providing a more secure pseudo-random binary sequence generators by using an internal control mechanism which is easy to implement (Puhl: Column 1 – 3 and Column 5 Line 34 – 37).

Accordingly, Becker as modified teaches the output sequence is randomly selected by applying one of the second plurality of binary sequences to a shift register (Puhl: Figure 2 Element 268; Beker: Figure 3: connecting the output of switch / MUX into the input of controller – i.e. LOAD signal as shown in Beker's Figure 3; Roth: Figure 5).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100